_TACTICAL THREAT INTELLIGENCE REPORT

Q4 2023

HOXHUNT

TABLE OF CONTENTS

Executive Summary

Hoxhunt's Threat Intelligence Report offers **a comprehensive overview on the phishing threat landscape during the final quarter of 2023**. It reveals insights into the evolving landscape of cyber threats by highlighting the tactics, techniques and procedures employed by threat actors.

The report showcases the largest phishing campaigns identified within the Hoxhunt network during Q4, including Microsoft and DocuSign impersonations. There is also an overview of two notable phishing campaigns targeting human error: malicious actors using compromised Booking.com accounts to send phishing messages and a BazarCall phishing campaign sending fake subscription renewal notices. Many of these campaigns demonstrate sophisticated social engineering techniques, often utilizing urgency and authority to manipulate recipients.

Most of the notable techniques being used by malicious actors involve spam filter bypassing, such as Bayesian poisoning and using clickable images as the email body. This means that **the technical firewall has failed and it's up to the humans to recognize phishing attempts.** Another commonly used technique, Adversary-in-the-Middle credential harvesters, allows malicious actors to bypass multifactor authentication.

Alongside these techniques, we consider **other technological and industry advancements and the effect they have on the importance of human risk management.** With the help of AI and Cybercrime-as-a-Service tools, crafting convincing spear phishing campaigns now requires significantly less effort. A malicious campaign can be launched by individuals with almost no technical skills, and deepfakes – images, voicemails, videos – are becoming more convincing. Attackers are also increasingly utilizing information they can legally find on social media services like LinkedIn to create better spear-phishing campaigns. Therefore, **human risk management is ever more important for mitigating cyber threats in organizations.**

Most of the notable techniques we spotted being used by malicious actors involve spam filter bypassing. This means that the technical firewall has failed and it's up to the humans to recognize phishing attempts.

About the authors

Hoxhunt is the leading platform for human cyber-risk management. Our solution goes beyond security awareness to drive behavior change and measurably lower human cyber-risk. Combining AI and behavioral science, we create individualized training moments people love.

Hoxhunt works with leading global companies such as Airbus, IGT, DocuSign, Nokia, AES, Avanade, and Kärcher and partners with global cybersecurity companies such as Microsoft and Deloitte.

Hoxhunt's Threat Operations Team consists of threat analysts and data scientists tasked with handling the emails reported to Hoxhunt.

During Q4 2023, around one million email threats were reported by our end users, averaging almost 10,000 reports per day. Because our end users manually report the emails, our data only consists of threats that have managed to bypass email spam filters. This data is analyzed by the Threat Operations team and combined with other data sources to create actionable intelligence.

www.hoxhunt.com

SUBSCRIBE TO OUR THREAT FEED

Hoxhunt's weekly threat feed showcases different phishing campaigns we have seen in the Hoxhunt network.

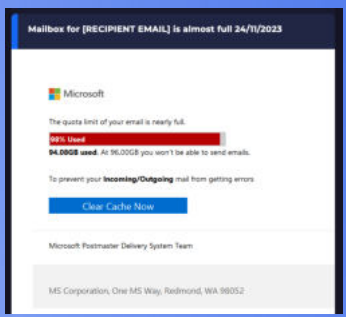
NOTABLE CAMPAIGNS

Largest threat campaigns

SUBSCRIBE TO OUR THREAT FEED

Hoxhunt's weekly threat feed showcases different phishing campaigns we have seen in the Hoxhunt network. Here are some highlights of the largest campaigns of Q4.

_01



MICROSOFT IMPERSONATION: MAILBOX IS ALMOST FULL

Payload: Malicious link

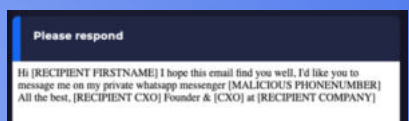
This is a classic Microsoft impersonation. The recipient is told that their mailbox is almost full and they must clear their cache now to avoid errors. Malicious actors are using urgency to social engineer the recipient to click the provided malicious link. This campaign uses a spam filter bypassing technique: the email body is an image with an embedded hyperlink, which doesn't contain any text for a filter to pick up.

CXO IMPERSONATION: PLEASE MESSAGE ME ON MY PRIVATE NUMBER

Payload: Pretext

This CXO impersonation is trying to get the recipient to message the provided phone number. The email uses automated personalization and includes details such as the recipient's company and their real CXO's name. This email is an example of authority impersonation, which as a social engineering tactic makes the recipient more likely to act on the email.

_02

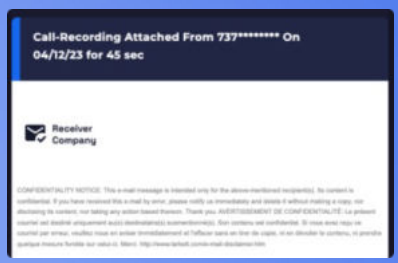


Largest threat campaigns

SUBSCRIBE TO OUR THREAT FEED

Hoxhunt's weekly threat feed showcases different phishing campaigns we have seen in the Hoxhunt network. Here are some highlights of the largest campaigns of Q4.

_03



FAKE VOICEMAIL NOTIFICATION

Payload: Malicious attachment

This phishing email is a fake voice mail notification. These kinds of notifications are a common phishing scheme. The easiest way to recognize these as malicious is to check the attachment filetype. A legitimate message would contain an audio file, such as .wav or .mp3.

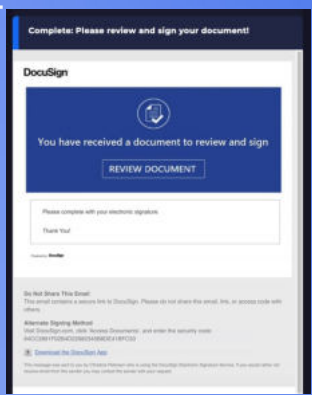
This campaign also uses Bayesian poisoning to bypass the spam filter. The email body itself doesn't have any text, so malicious actors have added an unrelated confidentiality footer to the bottom to make the email less suspicious to the spam filter.

DOCUSIGN IMPERSONATION: PLEASE REVIEW AND SIGN YOUR DOCUMENT

Payload: Malicious link

This phishing email is impersonating DocuSign. It claims the recipient has received a document that must be reviewed and signed. The email is very generic, which makes the template very reusable. This campaign uses a spam filter bypassing technique: the email body is an image with a hyperlink embedded in it and doesn't contain any text for a filter to pick up.

_04



Noteworthy campaigns

We have selected two campaigns to showcase how malicious actors have utilized human error as the initial attack vector. The first campaign is multi-step and involves compromising the Booking.com accounts of hotels to send phishing messages to users that have bookings at the hotel. The second one involves sending fake subscription renewal notices to users with the goal of getting the recipient to call a malicious number to cancel the subscription. Both campaigns use social engineering to get the recipients to interact with the emails.

BOOKING.COM CAMPAIGN

Step 1: Establish contact

Malicious actors compromise Booking.com accounts by creating hotel bookings and replying to the automatic confirmation message. The themes of the messages are often related to lost passports, elderly parents, anniversaries and navigation problems. This establish contact with the target, a Booking.com representative.

Step 2: Deliver malware, acquire credentials

After forming contact, the malicious actor sends a follow up message with infostealer malware. When executed, the malware steals passwords from the host. In this campaign, the target is specifically the hotel's Booking.com account credentials

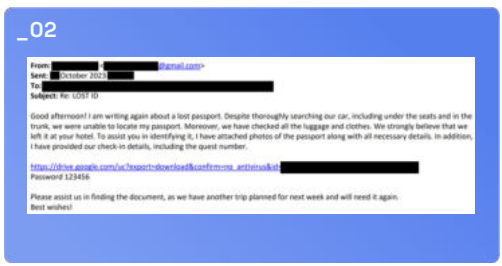
Step 3: Send notifications with malicious links

After gaining access to the Booking.com account, the malicious actor sends legitimate notifications to users with bookings at the hotel. These notifications appear otherwise legitimate but include malicious links within the message field.

The campaign utilizes the trust users have in Booking.com as both a sender and a service. Compromising legitimate accounts has two benefits for the malicious actors: they gain access to a list of targets (users with bookings at the hotel) and gain a delivery method for the malicious content (sending notifications related to the bookings).

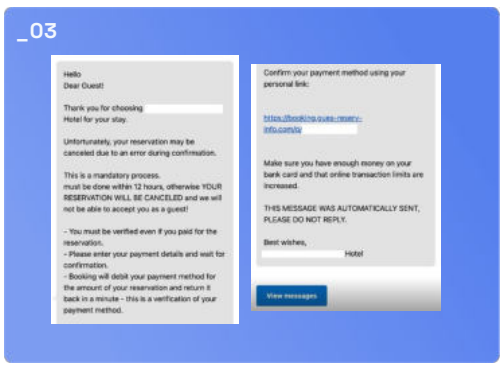
In phishing, context is key. This is visible in both parts of the campaign: in the first part, the hotel representative thinks they are interacting with a legitimate customer that has a problem, and in the second part, the recipient thinks there is a problem with the hotel booking and that the hotel is trying to help them.

Initial email. Source: Secureworks



Follow-up email. Source: Secureworks

When executed, the malware steals passwords from the host, and in this campaign the target is specifically the hotels Booking.com account credentials.



If the user clicks on the link, they are taken to a look-a-like Booking.com website that asks for their personal and financial information.

Noteworthy campaigns

BAZARCALL PHISHING CAMPAIGNS

BazarCall callback phishing attacks were first observed in late 2020. The campaign uses phishing messages that impersonate different services and inform the recipient that a subscription is about to be renewed. The impersonated services include eBay, PayPal, QuickBooks, McAfee, Disney+, and GeekSquad. The message contains a malicious phone number the recipient must call to cancel the subscription. If the recipient does call the number, the threat actors will attempt to social engineer them to download malware onto their device.

We have been receiving reports of BazarCall emails since 2021. Visually the emails have changed over the years, but the themes have stayed consistent. For example, GeekSquad subscriptions have remained popular.

The BazarCall campaign utilizes social engineering to get the recipient to call the provided number. This is done through creating an urgent scenario that must be acted upon (subscription cancellation), or the payment will go through.

Previously the emails in this campaign have been sent using free email providers such as Gmail, but recently HackerNews has reported that BazarCall has started utilizing Google Forms as a delivery method. This is a significant change in behavior, as previously most BazarCall phishing emails were sent using free email providers such as Gmail. Using Google Forms gives the messages additional legitimacy, as the sender appears to be Google.com.

An example of a GeekSquad BazarCall email from 2021

A GeekSquad from October 2023

INDUSTRY ADVANCEMENTS

Industry Advancements

QR code phishing was a big trend in 2023, and QR codes were used for many different campaigns as illustrated by our analysts in September. The trend continued in Q4: in October 2023, 22% of the phishing attacks rated by our analysts utilized QR codes.

Another continued trend was Cybercrime-as-a-Service (CaaS), which means that contrary to popular belief, launching cyber-attacks doesn't require advanced technical skills. These services are openly advertized, and the service providers even offer "customer" support. Specific services include **Ransomware-as-a-Service (RaaS),** which not only makes launching the attacks easier, but also "fosters economies of scale", according to an article by The Hacker News. For example, when specific ransomware is widely spread and the victim can find multiple reports of it, they feel more threatened and are more inclined to pay the ransom.

An anticipated big threat for 2024 is AI-based phishing, which utilizes **generative AI** in different ways to create convincing and sophisticated phishing campaigns. For example, AI tools help cybercriminals operate in all different languages, create fake selfies, craft malicious websites, generate audio, and help write malicious code. This not only makes it easier for malicious actors to create phishing campaigns, but also makes attacks harder to detect. Deepfakes can be used for impersonating executives to gain access to sensitive information and spreading political misinformation, and with 40 national elections in 2024 including the US presidential election, the latter will be something to look out for this coming year.

These industry advancements paint a picture of a constantly changing and evolving landscape. As a response**, to prevent successful phishing, human risk management and security training must be equally adaptable, comprehensive and quick to change.** Especially with the more and more convincing materials produced by AI, it is important to be increasingly critical of what can be read, heard or seen online.

Industries targeted

Based on our data and industry news, we've noticed that the following industries have been especially targeted by malicious actors:

- international affairs
- defense
- logistics
- academia
- information security
- technology
- cryptocurrency
- transportation
- energy
- military sectors
- maritime
- telecommunications
- consulting
- hospitality
- retail
- manufacturing
- law
- government agencies

Although the list seems very exhaustive, it highlights the fact that almost every single industry is targeted and should be prepared for this through proper security policies and culture.

We've also noticed there are specific job roles that are more targeted than others: individuals in sensitive roles, especially those employed by an organization in a more critical industry. This includes IT service providers, software developers, government officials, high-profile individuals, tech space employees, and recruitment & hiring staff. This highlights that companies should be aware of which employees are the most likely targets and prepare accordingly. This includes providing continuous and dynamic training.

HUMAN RISK NEWS

Human Risk News

When it comes to exploiting human risk, there were some worrisome news and developments in Q4. The frequency of **ransomware attacks** seemed to be breaking records in 2023, increasing by 37% compared to 2022, while the use of phishing as an email attack technique has also gained further popularity.

Spear-phishing as a way to gain initial access remains popular, made easier by social media "oversharing" and the possibilities of AI. For example, cybercriminals might access personal data on LinkedIn, allowing for more **specific and believable social engineering attacks.** In a way, LinkedIn is a gold mine for attackers, as it is by nature a place where people share quite openly, and accept "Connect" requests with less hesitation, perhaps, than friend requests on Facebook. **In addition to intelligence gathering, attackers have used LinkedIn to carry out attacks**, for example posing as recruiters. It's important to stay vigilant on social media services and to understand what personal information is publicly available, and how that information might be used for social engineering.

While AI has a lot to offer for doing good, it can also be used maliciously. This is true for phishing as well. Tools such as **WormGPT** and **FraudGPT** help write malicious code and even analyze vulnerabilities of IT systems, and they can also be used for crafting convincing spear-phishing emails at a large scale.

Furthermore, it's expected that AI-based voice mail phishing, *vishing*, will gain popularity in 2024. With **more convincing deepfake audios and more sophisticated large language models**, it is possible to carry out malicious conversations with victims without a human threat actor interference.

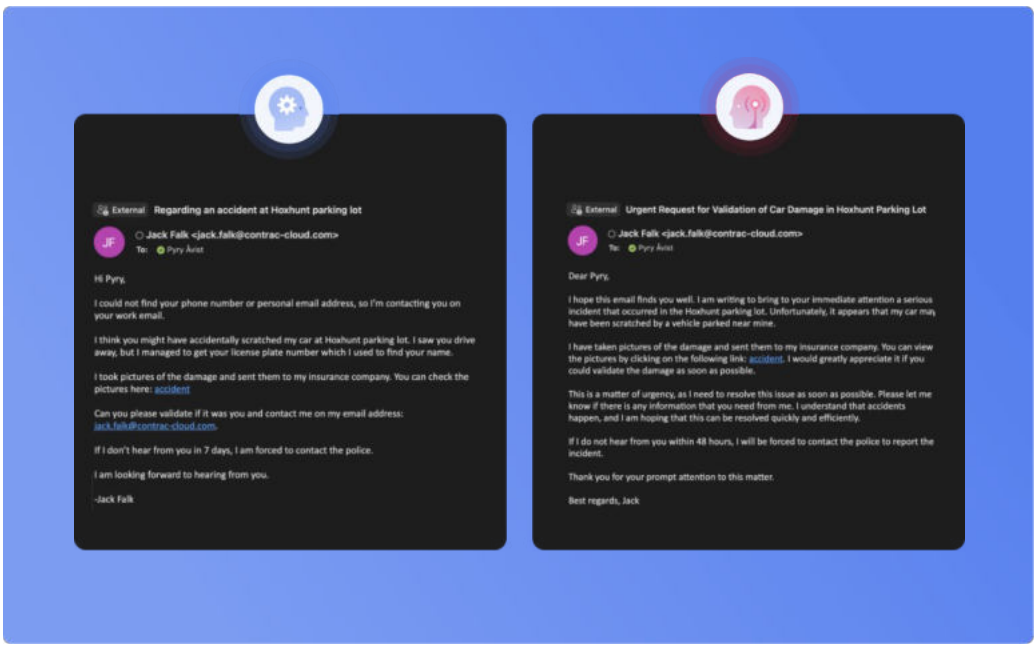
These developments show the value of investing and prioritizing cybersecurity training to mitigate possible threats, whether campaigns are crafted by a human or AI. According to the article Are We Ready to Give Up on Security Awareness Training (16th of November, 2023) by The Hacker News, **future cybersecurity training is expected to be "short, designed for different levels security expertise, and accessible".** This allows for training to be easily implemented and its content to be better remembered in day-to-day work, unlike longer and less engaging training sessions.

In early 2023, we conducted an experiment to see who's better at phishing: humans or ChatGPT.

In the beginning of 2023, we conducted an experiment to see who's better at phishing: humans or ChatGPT. The email on the left is created by our social engineer, and the one on the right by ChatGPT.

The results showed that humans are still better at social engineering than AI, outperforming ChatGPT by around 45%. Nevertheless, AI allows for large-scale spear-phishing campaigns, and the development of malicious tools like WormGPT and FraudGPT can amplify the threat of generative AI.

Read the full study on our website.



TACTICS, TECHNIQUES, AND PROCEDURES

Tactics, Techniques, and Procedures

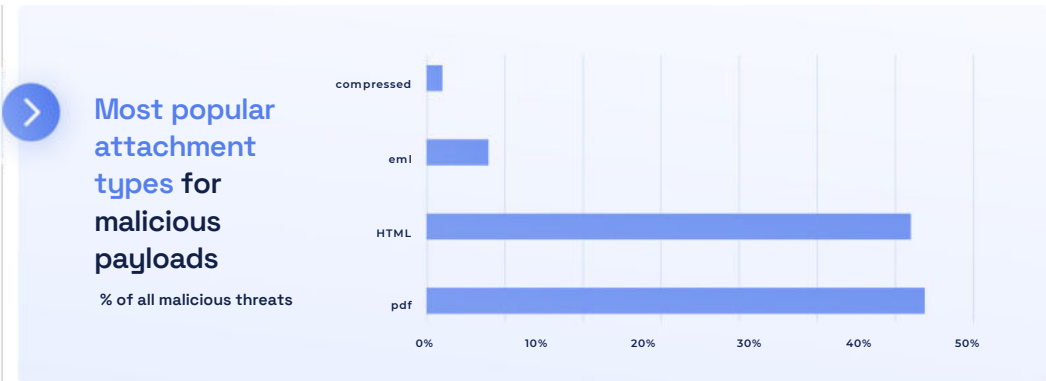
File extensions used as malicious attachments

PDFs are the most popular file type used in malicious attachments. They often include a link to a further payload, which could be another download or a credential harvester.

HTML files are the second most popular file type and compared to PDFs, HTML files are mainly used as credential harvesters.

The third most popular attachment type is eml files, which are emails saved in plain text. Malicious actors use this technique to smuggle phishing emails through email filter as eml attachments within innocent looking emails.

The **fourth most popular attachment type is compressed files**. Malicious actors can compress their payloads to make it more difficult for both humans and email filters to identify.

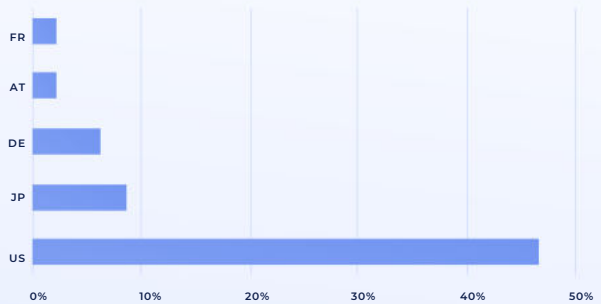


Tactics, Techniques, and Procedures

Origins of malicious threats

Using our data, we have identified **the US as the most prominent origin for malicious threats** that have been reported to us. Approximately 45% of the threats we receive have seemingly originated from the US. The second highest is Japan at a bit less than 10%, followed by Germany, Austria and France. This data is based on IP and email routing information analysis of malicious threats reported to Hoxhunt.

Top five origin countries for malicious threats

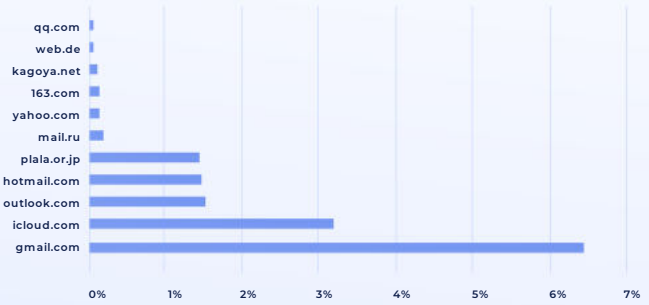


Most popular free sender domains

Free web-based email services located in the US are the most common free sender domains used to send malicious threats. Following them, Japan based plala.org.jp is the next highest. These are then followed by a variety of smaller domestic email services such as mail.ru, web.de and qq.com.

Top free sender domains used to send malicious threats

% of all malicious threats

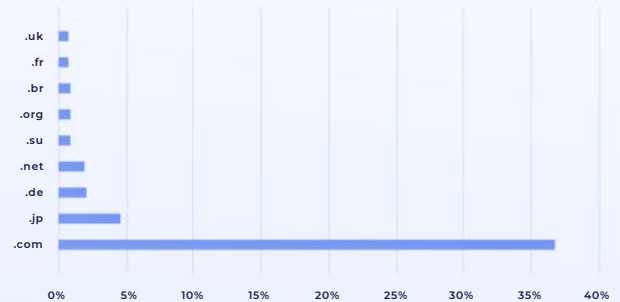


Tactics, Techniques, and Procedures

Most popular top-level domains (TLDs)

Related to the earlier statistic on free sender domains, the most popular TLD used to send malicious threats is *.com*. Following this *.jp* is the second highest, partly due to the popularity of plala.or.jp as a webmail provider used by malicious actors.

Most popular top-level domains (TLDs) used to send malicious threats

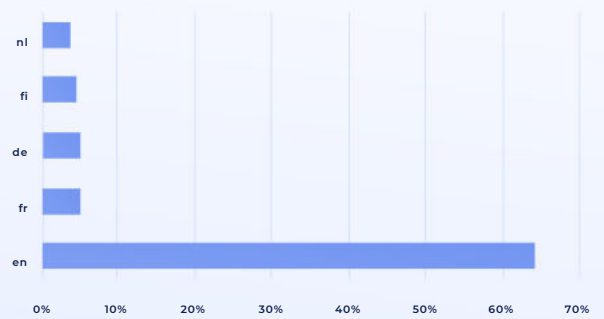


Languages used in malicious threats

Over 60% of all malicious threats reported within the Hoxhunt network in Q4 were in English. The other top four languages were French, German, Finnish and Dutch*, each between 3–5% of the total. This highlights that **English is by far the most popular language used in phishing.**

** The data may be skewed due to a large percentage of European end users.*

Top five languages used in malicious threats



Tactics, Techniques, and Procedures

Popular techniques used by malicious actors

We've identified three main techniques used by malicious actors in this quarter. The first two are both related to bypassing spam filters: **Bayesian poisoning and using only images with hyperlinks within the email body.** These highlight how malicious actors change their methodologies as spam filters evolve to bypass them. When the technical layer fails to identify the threat, it is up to the human to rise to the occasion.

The third technique we've identified is Adversary-in-the-Middle credential harvesters. **21,4% of credential harvesters used in phishing attacks studied during Dec 2023 and Jan 2024 were AitM capable.**

Technique: Email body is a clickable image

A popular technique used to bypass spam filters is to not include any text in the email. This makes it harder for the filter to recognize a message as spam, because there are no words to analyze.

Using only a clickable image in the email body is a technique that allows the malicious actors to avoid using words in the email body. The email visually looks the same as a regular email, but instead of having regular content, the email body is just an image with a hyperlink embedded into it.

We see this most often being done in low quality bulk phishing campaigns such as Microsoft impersonations and DocuSign impersonations.

Tactics, Techniques, and Procedures

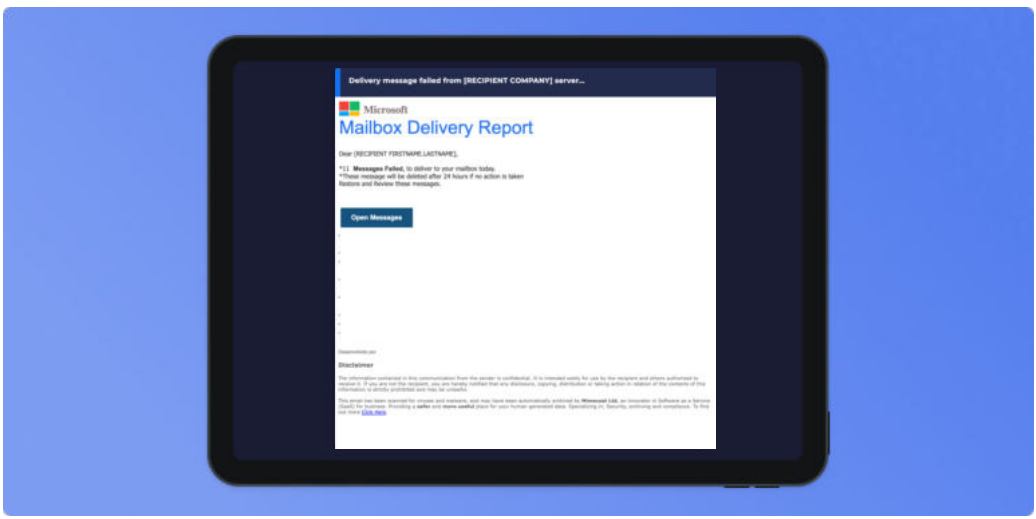
Technique: Bayesian poisoning

A popular technique used to bypass spam filters in Q4 of 2023 was Bayesian poisoning. Many email filters use Bayesian filtering to check incoming emails for spam, which checks incoming emails for specific words. These words are then used to calculate the probability of the message being spam. The filter is capable of learning from messages that were identified as spam and messages that were identified as not being spam.

Bayesian poisoning is a technique that allows malicious actors to bypass Bayesian spam filters. This is done by adding unrelated text to the email body. The extra text adds additional words which the Bayesian spam filter will see and use to decide whether a message is spam or not. Sometimes the additional text is hidden in the body so that it is only visible to the email filter.

In our data, we have identified a few different methods malicious actors have used for Bayesian poisoning.

The most popular one currently is to add confidentiality disclaimers at the bottom of emails. They are often unrelated to the message itself and are copied from a variety of different companies and services. Other methods identified include adding unrelated email conversations and contents lists from different sources.



Tactics, Techniques, and Procedures

Technique: Adversary-in-the-Middle (AitM)

AitM credential harvesters are advanced and capable of harvesting MFA and session tokens. As the name suggests, the basic premise is that the adversary is between the end user and the legitimate website they wish to access.

This can be achieved through a variety of ways, but a basic one would be the adversary showing a streamed version of a login page to the end user. The real login page is on the adversary's device, and when the end user inputs their credentials, they are actually logging into the service on the adversary's device. If the account has MFA set up on it, the user will accept the authentication prompt because they think they are logging into the legitimate service. Unfortunately, the prompt is for the adversary's device, and accepting the prompt gives them access to the account.

21,4% of credential harvesters used in phishing attacks studied during Dec 2023 and Jan 2024 were AitM capable